IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
ROANOKE DIVISION

UNITED STATES OF AMERICA,	)	Case No. 7:22-cr-00001
	)	
v.	)	**MEMORANDUM OPINION**
	)	
JERALD GRAY,	)	By: Hon. Thomas T. Cullen
	)	United States District Judge
Defendant.	)	

Defendant Jerald Gray, who is currently charged with unlawful possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B), moves to suppress evidence obtained by federal agents during a search of computers in his home. This search was conducted pursuant to a warrant issued by a federal magistrate judge. In support of his motion, Gray contends that the lead agent—and search warrant affiant—omitted specific details from the probable cause affidavit about an algorithm that she had utilized to determine that Gray's computer had requested three images of child pornography from the computer network known as Freenet. Specifically, Gray contends that this omission was intentional because the algorithm, which is discussed at length in the affidavit, "appears farcical." (Def.'s Mot. to Suppress at 3 [ECF No. 84].) But Gray provides no evidence to back up this startling claim. In addition, Gray contends that the affidavit, in its current form, fails to establish probable cause to justify the search. As discussed below, both arguments lack merit, and the court will deny the motion.

I. BACKGROUND

Magistrate Judge Robert Ballou signed the warrant at issue on December 3, 2021, based on the 36-page affidavit of Special Agent ("SA") Kathryn Weber, a veteran FBI agent with experience and specialized training investigating crimes against children. (*See* Gov.'s Ex. 1 ¶ 1 [ECF No. 85-1].) As set forth in SA Weber's affidavit, her investigation involved Gray's alleged use of Freenet to obtain child pornography. Freenet, a peer-to-peer file-sharing network that is designed to afford anonymity to its users, was developed by computer scientists at the advent of the Internet age. It is well known—both to consumers of child pornography as well as to law enforcement officials, who routinely conduct undercover surveillance of suspected child pornography on this public forum. [1]

According to SA Weber, a Freenet user who downloads the software and elects to peruse the network in its default "Opennet" mode is automatically connected to a fixed number of "peers," or other computers hosting the same software in Opennet form. Although this Freenet user can see the Internet Protocol ("IP") addresses of his peers, their identities are otherwise unknown to him. (*Id.* ¶¶ 8–9.) The number of peers a particular Freenet user has at any given time varies and is determined by, among other things, Internet speed. (*Id.* ¶ 8, n.1.) As a condition of using the Freenet software, each user agrees to dedicate a portion of his computer's hard drive to store small pieces of encrypted files called "blocks." (*Id.* ¶ 9.)

[1] Gray does not dispute the government's characterization, as detailed in the search warrant affidavit, of how Freenet works or the intricate process by which files are transferred among its users. Indeed, numerous courts have made nearly identical factual findings about the design and inner workings of Freenet. *See,* e.g., *United States v. Weyerman*, No. 21-1896, 2022 WL 1552997, at *1 (3d Cir. May 17, 2022) ("Freenet attempts to hide the identity of the original requester by making it difficult to differentiate whether a request for a piece that comes in from a peer originated with that peer . . . or whether that peer was simply forwarding a different peer's request." (cleaned up); *United States v. Dickerman*, 954 F.3d 1060, 1064 (8th Cir. 2020) ("Freenet's ability to hide what a user is requesting from the network has attracted persons that wish to collect and/or share child pornography files.") (cleaned up); *United States v. Pobre*, No. 8:19-CR-348-PX, 2022 WL 1136891, at *2 (D. Md. Apr. 15, 2022) (finding that Freenet configures and stores content in such a way that no single computer can be said to possess any given file, until a user downloads a manifest key that indexes all blocks associated with the file, by linking computers to each other and breaking up each uploaded file into encrypted blocks).

When a Freenet user uploads a file onto the network, the software breaks up that file into blocks and disseminates these blocks across the "Freenet network of peers." (*Id.* ¶ 9.) To download a particular file from the network, a Freenet user must first obtain a key—a series of letters, numbers, and special characters. These keys, along with descriptions of the encrypted files, can be obtained from Freenet's message boards and myriad other sources. (*See id.* ¶ 9–10.)

According to SA Weber's affidavit, once a user obtains the key for a desired file, he can begin the downloading process. (*Id.* ¶ 10.) Because encrypted blocks of the requested file are scattered across the entire network, this process involves sending numerous requests for these blocks—first, to the requestor's peers and, if they don't have the requested blocks, to the peers of the requestor's peers. (*Id.* ¶ 11.) As the affidavit explains, "Rather than request all of the file pieces from a single peer, requests for file pieces are divided up in roughly equal amounts among the user's peers. (*Id.*) If a user's peer does not have the particular requested pieces in its storage, that peer will then divide up and ask its peers for the pieces, and so on." (*Id.*)

Freenet attempts to conceal the identity of the peer who originally requested the file by making it difficult "to differentiate whether a request for a piece that comes in from a peer originated with that peer (i.e., the peer was the 'original requestor' of the file), or whether that peer was simply forwarding a different peer's request." (*Id.* ¶ 13.) It does this by "randomizing the initial number of times a request can be forwarded from one peer to another to be either 17 or 18. (*Id.*) Without this randomization, any time a user received a request for a piece of a file that could be forwarded 18 times, the user would know that its peer was the original requestor." (*Id.*)

Given these unique anonymizing features and the software's wide availability, Freenet is rife with child pornography. It is no surprise then that law enforcement has been actively monitoring this platform for the past 10 years, using undercover computers running modified Freenet software and logging requests for documented images of child pornography. (*Id.* ¶ 20.) Professors from the University of Massachusetts at Amherst and the Rochester Institute of Technology substantially aided these efforts by developing an algorithm that predicts, with better than 98 percent accuracy[2], whether a Freenet request for blocks of a file is the original request or merely a relayed request.[3] The details of this complex mathematical formula are beyond the court's complete comprehension, but, as the government explains, the algorithm makes logical deductions based on publicly available data associated with each request—namely, the number of the requester's peers and the number of requests that requestor made to the undercover computer.[4] (Gov.'s Resp. to Mot. to Suppress at 3 [ECF No. 85].) Simply put, because Freenet's default settings divide original requests almost evenly among the requestor's peers, and because subsequent, or relayed, requests from those peers involve a

[2] *See Pobre*, 2022 WL 1136891, at *3 ("the algorithm ascertains with over 98% probability whether the identified block request came from an original requesting node"); *United States v. Sigouin*, 494 F. Supp. 3d 1252, 1268 (S.D. Fla. 2019) (finding a false positive rate of 2%); *United States v. Dickerman*, 954 F.3d 1060, 1063 (8th Cir. 2020) ("The algorithm allows law enforcement to distinguish between requests sent from an original requester and requests forwarded by a relayer.").

[3] (*See* Brian N. Levine & Brian Lynn, *A Forensically Sound Method of Identifying Downloaders and Uploaders in Freenet*, Nov. 9–13, 2020 CCS 1497, 1500 (2020) [ECF No. 85-3].) The algorithm is contained in this peer-reviewed and publicly available academic paper.

[4] The algorithm's principal developer, Dr. Brian Levine, recently testified in two cases about how the algorithm works. *See United States v. Weyerman*, Crim. No. 19-88 (E.D. Pa. Jan. 3, 2020), aff'd, No. 21-1896, 2022 WL 1552997, at *1 (3d Cir. May 17, 2022); *United States v. Dickerman*, No. 416CR00258HEANAB1, 2017 WL 11485604, *1 (E.D. Mo. Sept. 26, 2017), report and recommendation adopted, No. 4:16CR258 HEA, 2018 WL 10228437 (E.D. Mo. Apr. 27, 2018), aff'd, 954 F.3d 1060 (8th Cir. 2020).

much smaller number of blocks, the algorithm accurately deduces whether a particular computer is the likely original requestor. (*See id.* at 3.) And because every Freenet user can see the IP addresses of his peers, law enforcement users can record the IP addresses of peers that, based on the algorithm, are likely original requestors of known child pornography.

According to SA Weber's affidavit, this is precisely how Gray landed on the FBI's radar. In July and August of 2021, a computer with an IP address that agents later determined was registered in Gray's name and associated with his residence in Covington, Virginia, made three separate requests for blocks of three files known by law enforcement to be child pornography. (*Id.* at 4; Gov.'s Ex. 1 ¶¶ 26-29.) Unbeknownst to this user (allegedly Gray), one of his peers on each of these three occasions was an FBI computer running Freenet software. Based on the number of blocks requested, the total number of file blocks required to reconstruct the file images, and the number of peers the target user had on each occasion, SA Weber, relying on the algorithm, determined that the user likely "was the original requestor of each of the described files." (Gov.'s Ex. 1 ¶ 26.) The agent then applied for a search warrant for Gray's residence and any electronic devices located there. Law enforcement executed this search warrant in early December 2021, and that search uncovered a plethora of child pornography on Gray's computer. (Gov.'s Resp. to Mot. to Suppress at 4.)

II. ANALYSIS

As noted above, Gray essentially challenges the search on two grounds. First, he contends that the affiant withheld "key information necessary for the Magistrate to conduct an independent assessment of probable cause." (Def.'s Mot. to Suppress at 5.) In support of this argument, Gray asserts that the algorithm at issue "appears farcical," and that the government duped the magistrate judge into believing that it is based on valid and reliable mathematical principles. Gray, in other words, argues that the government has committed a so-called *Franks* violation, justifying an evidentiary hearing.[5] Second, Gray asserts that the affidavit, on its face, fails to establish probable cause. Specifically, he argues that the affidavit lacked detailed information about how the algorithm led law enforcement to the conclusion that his computer was the original requestor of the illicit files at issue.

A. Alleged *Franks* Violation

"An accused is generally not entitled to challenge the veracity of a facially valid search warrant affidavit." *United States v. Allen*, 631 F.3d 164, 171 (4th Cir. 2011). But a *Franks* hearing "provides a criminal defendant with a narrow way to attack the validity of an affidavit." *United States v. Moody*, 931 F.3d 366, 370 (4th Cir. 2019). To obtain an evidentiary hearing, a defendant must make a "substantial preliminary showing" that the government made a false statement in the warrant affidavit; that the false statement was made knowingly and intentionally; and that it was material—i.e., that it was essential to the finding of probable cause.[6] *United States v. White*, 850 F.3d 667, 673 (4th Cir. 2017) (citing *Franks*, 438 U.S. at 155–56). "The first required showing, of falsity, cannot be conclusory and must rest on affidavits and other evidence." *Moody*, 931 F.3d at 370. In other words, the defendant "cannot rely on purely subjective disagreement" over how the affidavit characterizes the facts; he must put forth

[5] These hearings are named for the Supreme Court's decision in *Franks v. Delaware*, 438 U.S. 154 (1978).

[6] *Franks* also protects against intentional or reckless omissions of material facts from search warrant affidavits. "When a defendant relies on an omission, this heavy burden is even harder to meet." *United States v. Haas*, 986 F.3d 467, 474 (4th Cir. 2021). The defendant must make a substantial preliminary showing that (1) law enforcement made an omission; (2) it made the admission knowingly or recklessly; and (3) the inclusion of the omitted material would have defeated probable cause. *Id.*

actual evidence "showing that the statements at issue are objectively false." *Id.*; s*ee also Franks*, 438 U.S. at 171 (the defendant's "attack must be more than conclusory and must be supported by more than a mere desire to cross-examine").

Gray's contention that the algorithm "appears farcical" implies that SA Weber lied when she represented that the algorithm helped her to determine that he was the original requestor of files containing known child pornography. But one can also read Gray's argument to suggest that the government is guilty of making a material omission—namely that it intentionally omitted certain (unspecified) details about the algorithm that, if disclosed, would have defeated probable cause. Whether Gray is alleging falsity or omission makes no difference; he has put forth zero evidence to support either claim. Specifically, he has not proffered or cited any evidence, through affidavits or otherwise, that challenges any of the detailed factual assertions and explanations in the affidavit about the Freenet algorithm generally, or how it was applied in this case. Accordingly, Gray's contentions are paradigmatic of the kind of conclusory allegations that courts have long held are insufficient to trigger an evidentiary hearing on the validity of a search warrant. *See, e.g., Haas*, 986 F.3d at 477 ("Because Haas failed to make a substantial preliminary showing that the agent acted with the requisite intent in omitting Sarah's criminal history from the warrant affidavits, we affirm the district court's denial of Hass's requests for a *Franks* hearing."); *United States v. Seigler*, 990 F.3d 331, 344 (4th Cir. 2021) ("In short, there's no indication that this representation actually was false or misleading, that it was knowingly or recklessly so, or that it was the basis of the court's probable cause finding."); *Moody*, 931 F.3d at 374 ("A defendant must meet a high bar before he may challenge the veracity of a facially valid search warrant."). The court will therefore deny Gray's motion, insofar as he seeks an evidentiary hearing based on an alleged *Franks* violation.

B. Probable Cause

Gray also argues that the affidavit, in its original form, failed to establish probable cause for the search. The government must obtain a search warrant supported by probable cause prior to searching an individual's residence. *See* U.S. Const. amend. IV; *Fernandez v. California*, 571 U.S. 292, 298 (2014). "Probable cause requires only 'a fair probability,' and not a prima facie showing, that 'contraband or evidence of a crime will be found in a particular place.'" *United States v. Bosyk*, 933 F.3d 319, 325 (4th Cir. 2019) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). Probable cause, in other words, is "not a high bar," and law enforcement officers are not obligated to "rule out a suspect's innocent explanation for suspicious facts." *District of Columbia v. Wesby*, 138 S. Ct. 577, 588 (2018). This court reviews a magistrate judge's decision to issue a search warrant "with great deference, asking only whether the judicial officer had a substantial basis for finding probable cause." *United States v. Blakeney*, 949 F.3d 851, 859 (4th Cir. 2020) (cleaned up). In so doing, the court only considers the facts contained in the warrant affidavit.[7] *Bosyk*, 933 F.3d at 325 (citing *United States v. Lyles*, 910 F.3d 787, 791 (4th Cir. 2018)).

As noted above, Gray contends that the affidavit did not establish probable cause because it did not explain precisely how the Freenet algorithm pointed to him as the original requestor of three files containing known child pornography. Although the affidavit does not

[7] Because Gray is not entitled to an evidentiary hearing under *Franks*, and the court assesses his attendant probable-cause challenge solely based on the information presented in the affidavit, the court elects not to hold a hearing on this motion. In sum, the parties' arguments about the sufficiency of the information contained in the affidavit are adequately set forth in their written submissions, and oral argument would not aid the decisional process.

describe, with mathematical details, how the algorithm applies to the specific file requests in this case, this does not mean that it lacked probable cause. As noted above, the affidavit discussed, in detail, the development and general operation of Freenet, including how files are broken up and encrypted, and how users request and transfer file blocks among their first- and second-line peers. In addition, SA Weber explained how a computer directly linked to the defendant's IP address made *three separate requests* for files containing known child pornography. The affidavit further described the Freenet algorithm, including when and how it was developed, how it works in the typical case, and its general reliability. Specifically, the affidavit represented that the algorithm is highly accurate based on the results of a peer-reviewed study—a copy of which SA Weber noted was available for the magistrate judge's review upon request—and the agents' personal knowledge of its successful use in other cases. Finally, the affidavit explained that, after applying the algorithm's methodology to "the number of requested file pieces, the total number of file pieces required to assemble the file, and the number of peers that the user had," she concluded that Gray was likely the original requestor.

This information, considered in its totality, undoubtedly established a fair probability that computers associated with Gray's IP address would contain evidence of child pornography. And this is all that was required to justify the issuance of a search warrant. Although SA Weber could have provided the specific details of her algorithmic reasoning or attached a copy of the peer-reviewed study as an exhibit to the affidavit, her failure to do so does not change the outcome. Indeed, the detailed information and explanation that she did provide was more than sufficient to clear the relatively low bar of probable cause. *See Bosyk*, 933 F.3d at 332 (cleaned up) ("A warrant application is judged on the adequacy of what it does contain, not on what it lacks, or on what a critic might say should have been added.").

C. Good Faith Exception

Even if SA Weber's affidavit did not support Magistrate Judge Ballou's finding of probable cause, the good faith exception would prevent the court from excluding the evidence of child pornography found on Gray's computers. The exclusionary rule "bars the prosecution from introducing evidence obtained by way of a Fourth Amendment violation." *Davis v. United States*, 564 U.S. 229, 232 (2011). But under the good faith exception, "evidence seized in reasonable, good-faith reliance on a search warrant that is subsequently held to be defective is not subject to suppression, despite the existence of a constitutional violation." *United States v. Brunson*, 968 F.3d 325, 334 (4th Cir. 2020) (cleaned up). Courts have recognized four scenarios when the good faith exception will not apply: (1) when the magistrate judge is misled by information in a search warrant affidavit that the agent knew was false or would have known was false but for the agent's reckless disregard for the truth; (2) when the magistrate judge "wholly abandoned his judicial role"; (3) when the affidavit is so "lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; and (4) when the warrant is "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *United States v. Doyle*, 650 F.3d 460, 467 (4th Cir. 2011).

Gray only makes passing reference to the good faith exception, asserting, with little explanation, that it should not apply. Although vague, Gray suggests that because SA Weber did not include the algorithm itself within the body of the search warrant affidavit—the same algorithm that he also baldly asserts "appears farcical"—the government intentionally misled Judge Ballou. This suggestion that the first exception applies misses the mark. As explained above, Gray failed to offer even a scintilla of evidentiary support for his assertion that the Freenet algorithm is unreliable, let alone farcical. Without such evidence, the court is constrained to conclude that SA Weber's detailed assertions about the algorithm and its application in this case are true and correct and, thus, that the magistrate judge was not misled. Accordingly, the good faith exception would apply even if the warrant at issue had lacked probable cause.

III. Conclusion

For these reasons, the court will deny Defendant's motion.

The clerk is directed to forward a copy of this Memorandum Opinion and accompanying Order to all counsel of record.

ENTERED this 20th day of October, 2022.

/s/ Thomas T. Cullen
HON. THOMAS T. CULLEN
UNITED STATES DISTRICT JUDGE